ABSTRACT OF THE DISCLOSURE

Data is securely stored encrypted within a database server or portal within a public network. A wireless device first registers with an authentication center maintained separately from the database server to obtain a session key. The obtained session key is then used by the wireless device to request particular data from the database server. The database server, in response to said request, queries the authentication center to verify the authenticity of the wireless device. The authentication center verifies the received session key with the identified wireless device and provides the wireless device with a second group key. The authentication center further instructs the database server to comply with the data request and provide the wireless device with the encrypted data. The wireless device thereafter uses the received group key to decrypt the received data from the database server and is allowed access to the secured data.